ASSOCIATION OF METROPOLITAN WATER AGENCIES

LEADERS IN WATER

1620 I Street NW, Suite 500
Washington, DC 20006

P 202.505.1565
amwa.net

May 31, 2023

Via wicrd-outreach@epa.gov

Re: Comments on *Evaluating Cybersecurity During Public Water System Sanitary Surveys*

To Whom It May Concern:

The Association of Metropolitan Water Agencies (AMWA) appreciates the opportunity to provide these comments in response to the *Evaluating Cybersecurity During Public Water System Sanitary Surveys* guidance document published by EPA in conjunction with the release of its March 3, 2023 interpretive memorandum "Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process."

AMWA is an organization representing the largest publicly owned drinking water systems in the United States, and our member utilities generally serve populations of greater than 100,000 people. On behalf of our member public water systems, and as a partner organization of WaterISAC, we recognize the importance of ensuring that the water sector maintains a strong cyber posture and helping individual water systems take steps to prepare for and respond to cyber threats.

While the association has expressed concerns with the approach and validity of EPA's interpretive memorandum to require the inclusion of cybersecurity reviews in public water system sanitary surveys, these comments will generally be limited to the contents of sections 4 – 8 and the appendices of the guidance document. However, we do appreciate that section 3 of the guidance outlines different approaches that states may follow for evaluating cybersecurity at a PWS – including directing PWSs to undertake a self-assessment, or requiring PWS compliance with an alternative state program for water system cybersecurity. Provided that states can clearly articulate to PWSs what actions need to be taken to satisfactorily complete a self-assessment or comply with an alternative state program, we encourage EPA to widely promote these compliance options to states and PWSs.

In terms of the guidance to states that intend to conduct sanitary surveys with a new cybersecurity component, we believe the guidance document can be clarified for both public water systems subject to the expanded sanitary survey requirements, and state officials who will be charged with implementing them. This is especially important given that these new requirements will apply not only to the largest drinking water systems represented by AMWA, but also thousands of small public

water systems that may struggle to achieve compliance with the expanded scope of sanitary surveys. AMWA's specific observations and recommendations are explained below.

Section 4.2: Technical Assistance

Section 4.2 of the EPA document (Page 8) discusses a "Cybersecurity Technical Assistance Program for the Water Sector," through which states and public water systems can seek guidance from subject matter experts on questions such as "identifying whether a cybersecurity gap is a significant deficiency." However, Section 5.1 (Page 11) subsequently specifies that "the state is responsible for determining whether to designate a cybersecurity gap as a significant deficiency."

This prompts the question as to the degree to which public water systems should rely on guidance from the technical assistance program, especially if a subject matter expert indicates that a given cybersecurity gap does not constitute a significant deficiency. If the guidance is not the definitive answer to the question and could be contradicted by a state during a sanitary survey, then the value of the technical assistance is questionable. AMWA recommends that the technical assistance should be consistent with other similar materials offered through NIST and CISA, and that the guidance further clarify how subject matter experts will determine whether cybersecurity gaps constitute significant deficiencies, and how those findings will align with determinations made by states. Where there is disagreement, the guidance should explain how public water systems should best use the technical assistance provided by subject matter experts.

Section 4.3: Additional resources

Section 4.3 (Pages 8 – 10) list "additional technical and financial resources that can help states and PWSs with assessing cybersecurity during sanitary surveys." Among the resources referenced is WaterISAC, which the guidance describes as "a source for data, case studies, and analysis related to water security threats, including cyber-crime, and provides resources to support response, mitigation, and resilience initiatives." This is accurate, but it would be helpful to further note that WaterISAC is a nonprofit, dues-supported membership organization that public water systems must join in order to access its resources and benefits. Otherwise, a water system looking to quickly obtain information from WaterISAC based on the description in the guidance could encounter delays if it finds that it must first join the organization.

This section also lists several federal financial resources that PWSs may utilize to carry out cybersecurity improvements. Among them is EPA's Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program, which is designed to offer grants to support projects to address cyber and other vulnerabilities for PWSs serving communities of greater than 10,000 people. However, while Congress appropriated an initial $5 million for this program in the 2023 fiscal year, EPA has yet to offer any information about when it will be operational or what steps PWSs should take to apply for funds. Adding this information to the guidance when it is available will help eligible water systems utilize this important new resource to improve their cyber posture.

Section 6.0: Recommended alternatives to the EPA checklist

We appreciate that use of the specific EPA Checklist provided in the guidance is optional, and that a cybersecurity evaluation during a sanitary survey may utilize other assessment methods approved by the state. While the guidance specifically references several permissible assessment methods, it would be helpful if EPA defined baseline criteria representing components of a permissible method to ensure that all PWSs are evaluated consistently and against the same standards. This will also provide a consistent approach and response when technical assistance is requested.

Section 7.0: Potential significant deficiencies

This section (Pages 11 – 14) lists numerous "specific cybersecurity gaps" at PWSs that may be considered significant deficiencies, in the opinion of EPA. However, this section reiterates that "states retain their existing authority and discretion to determine when a cybersecurity gap … should be designated as a significant deficiency." This invites the question of whether states may only consider cybersecurity gaps specified in this section and in Appendix A, to constitute significant deficiencies, or if states may assign significant deficiencies based upon other, unlisted cybersecurity gaps. If it is the latter, then this guidance should be expanded to include every potential cyber-related significant deficiency possible to be identified by a state, so the public water system may have an opportunity to proactively address each of these gaps prior to a sanitary survey inspection.

AMWA also questions whether some of the potential cybersecurity gaps identified in this section may actually rise to the level of a PWS "significant deficiency" (defined by EPA as including, but not limited to, "defects in design, operation, or maintenance, or a failure or malfunction of the sources, treatment, storage, or distribution system that the state determines to be causing, or have potential for causing, the introduction of contamination into the water delivered to consumers.")[1] For example, while it may be a best practice for a PWS to "have a named role/position/title that is responsible for all … cybersecurity activities," or to "stipulate in its procurement documents that vendors and/or service providers shall [provide notice] of security incidents and confirmed vulnerabilities in a timely manner," the lack of either action does not necessarily have the potential to cause "the introduction of contamination into the water delivered to consumers." AMWA urges EPA to reiterate to states that only cybersecurity gaps with legitimate potential to directly cause the introduction of contamination into water delivered to consumers, or to otherwise cause a significant disruption to water services, should be considered a significant deficiency under the interpretive memorandum.

Section 8.0: How should states protect sensitive information on PWS cybersecurity?

AMWA agrees with EPA's contention that "withholding from public disclosure information about specific cybersecurity practices and vulnerabilities at PWSs may be necessary due to the potential for this information to be exploited to facilitate a cyber intrusion or attack on the PWS." However, the guidance and the larger interpretative memorandum ultimately leave it up to each state conducting a sanitary survey of a PWS to take necessary steps to ensure that this sensitive

[1] 40 CFR § 142.16(o)(2)(iv)

information does not fall into the wrong hands. This is especially concerning given that the guidance document acknowledges that "most" states have their own FOIA-like information protection laws in place.

Section 8.0 offers several potential strategies for states to avoid publicly disclosing sensitive public water system information encountered in the context of an expanded sanitary survey that includes a review of cybersecurity. These include state inspectors leaving cyber assessments in the possession of PWSs, limiting the contents of official reports, or placing "detailed notes on PWS cybersecurity vulnerabilities … in internal, non-public documents that are not subject to public disclosure requirements."

While these strategies are well-intentioned, they provide no guarantee that a state will not be required, under its own laws, to make public any information produced by its own inspectors during a sanitary survey inspection. They also leave unclear how a state may assess a significant deficiency against a PWS if a state is unable to possess information to justify that finding, or determine if a PWS has rectified it.

To address some of these issues, AMWA recommends that EPA should place clear and firm restrictions on the potentially sensitive cybersecurity data that may be generated during a sanitary survey. For example, all sensitive information should be kept with the PWS and not transferred to the state. We also favor clear and definitive requirements to be placed on surveyors regarding information collection, reporting, data submittal, and limitations on the content of notes that surveyors may take during inspections.

Appendix A: EPA Cybersecurity Checklist for Public Water System Sanitary Surveys

Finally, AMWA understands that Appendix A is intended to serve as a checklist that PWSs or states may use to conduct an assessment of recommended cybersecurity practices and controls. However, we request additional information from EPA on how a state would be able to evaluate whether a PWS has adequately implemented these practices.

For example, the Appendix A checklist recommends that a state evaluate whether a PWS may "detect and block repeated unsuccessful login attempts" (1.1), "change default passwords" (1.2), and "require approval before new software is installed or deployed" (2.1). What is unclear is how a state would accurately certify that a PWS has taken these steps in practice. Would a state inspector be granted access to a PWS's internal network in order to investigate and document software settings? Inviting a wide range of state inspectors to do so would introduce new security risks. Alternatively, if the guidance specified that it would be adequate for a state inspector to examine a logbook that verifies that password change or software installation had been carried out, this would provide more assurance that a PWS is carrying out these recommended actions, without granting the inspector access to the internal network.

Other items in the checklist may be difficult for a PWS to meet. For example, item 2.3 calls for a no-less-than-monthly review of all OT and IT network assets, and a list of all OT and IT assets with an IP address. But it is not clear how to implement this review for devices that are not on an IP network,

such as SCADA systems that use serial communications and therefore do not require the use of IP addresses. As an alternative, it may be effective for a water system to passively monitor all network traffic over a period of time to determine how "normal" traffic appears, and then identify when a discrepancy may indicate an incident of concern. Therefore, AMWA believes that a monthly confirmation by a PWS that a network is operating normally should meet the "review" requirement of item 2.3.

Additionally, item 2.5 directs PWSs to "maintain current documentation detailing the set-up and settings … of critical OT and IT assets." But it is not clear what constitutes "current" documentation. Would it be permissible for a public water system to update its set-up and settings documentation monthly, consistent with the asset review schedule in item 2.3?

Item number 7.3 further recommends that a PWS "maintain, store securely and separately, and test backups of critical PWA OT and IT systems." However, since older OT configurations may not be available and are constantly changing due to operational needs, having a robust disaster recovery plan that is validated regularly would be the best practice from an operational standpoint. We recommend that incorporating Consequent Driven Cyber Informed Engineering in the standard operating procedures – imagining the worst possible outcome of a cyber threat perpetrator, then building non-cyber or physical mitigation to lessen the possibility of a disaster occurring and separate and safeguard operations – should be part of design-builds moving forward.

Conclusion

AMWA appreciates the opportunity to comment on EPA's guidance document. We believe that the numerous questions and concerns we have raised about the document reflect our larger concerns about the wisdom and viability of attempting to use sanitary survey inspections as a means to review and enforce cybersecurity practices at PWSs. AMWA remains open to collaborate with EPA and other stakeholders and policymakers to develop a workable oversight mechanism to improve cybersecurity across the whole of the water sector.

Sincerely,

Thomas Dobbins
Chief Executive Officer